BY ORDER OF THE COMMANDER
AEROSPACE MAINTENANCE AND
REGENERATION CENTER

AMARC INSTRUCTION 33-114

1 AUGUST 2000

Communications and Information

SAFEGUARDING PERSONAL DATA IN AUTOMATED DATA PROCESSING SYSTEMS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the Davis-Montham AFB WWW site at: http:/ www.dm.af.mil/AMARC. If you lack access, contact your Publishing Distribution Office.

OPR: AMARC/XPI (M. Hulse)
Certified by: AMARC/XPI (J. Bohan)
Supersedes AMARCI 33-114, 14 August 1997
Pages: 3
Distribution: F

This instruction implements Air Force Policy Directive 33-1, *Command, Control, Communications and Computer (C4) Systems.* It is affected by the Privacy Act of 1974. Input and output products that are subject to AFI 37-132, *Air Force Privacy Act,* will have a Privacy Act Statement typed or stamped on each page of the product. This procedure applies to all AMARC personnel.

SUMMARY OF CHANGES: Changes were made to realign duties with organizational changes An asterisk (*) indicates a change from previous instruction.

1. GENERAL.

1.1. The privacy act requires each federal agency to take specific actions to safeguard any system of records with personal data and is designed to:

1.1.1. Allow individuals access to records kept by federal agencies which pertain to them.

1.1.2. Prevent a possible invasion of privacy by prohibiting unauthorized access to records that have personal data.

1.2. This instruction applies to those parts of the Privacy Act which pertain to ensuring the accuracy and confidentiality of personal data records in the AMARC automated data systems and to the identification, distribution, protection and destruction of these products in accordance with (IAW) AFI 33-132.

1.3. In performing their duties, some personnel have access via terminal or through printed output to data, such as social security account number (SSN), grade and step, leave records or wage tables which must be protected from unauthorized disclosure and alteration.

1.4. Criminal penalties and fines can be imposed on an individual who makes willful unauthorized disclosures of personal data or who obtains access to records under false pretenses.

2. RESPONSIBILITIES.

2.1. The Communication Management Division (XPI) (AMARC Information Systems Privacy Act Monitor) sets up local policy to enforce the provisions of the Privacy Act that pertains to automated systems.

2.2. XPI will ensure that:

2.2.1. In coordination with the functional office of primary responsibility (OPR) for each data system, all data products which must be protected are identified.

2.2.2. Each page of all lists which need protection has the phrase: "Personal Data - Privacy Act of 1974 (5 U. S. C. 522a)."

2.2.3. All test data have fictitious personal data (name and SSN).

2.2.4. Any system which has remote inquiry capability (by name and SSN) to records with personal data includes programmatic safeguards to prevent unauthorized interrogation or alteration of the records.

2.2.5. Each page of all Reports Generator Program lists which must be protected has the phrase Personal Data - Privacy Act of 1974 (5 U. S. C. 522a)."

2.2.6. Magnetic tapes, designated in XPI Operating Instructions as containing personal data, are safeguarded.

2.2.7. Internal records with personal data may be altered as follows; minor changes may be requested orally, but more serious requests shall be in writing. Changes should be completed within 30 days.

2.2.8. Input and output data products which must be safeguarded are processed IAW applicable XPI instructions and are protected from unauthorized disclosure while they are in the data entry area.

2.2.9. Policies for the physical protection of the data management controlled area are enforced to safeguard applicable data products while in XPI control.

2.2.10. Terminal access to personal data is limited to individuals identified in writing to XPI by division/branch chiefs.

3. PROCEDURES:

3.1. Each division/office will request access to personal data for employees via letter to XPI.

3.1.1. Requests for access to personal data via terminal must include the employee's name, office symbol, telephone and applicable work center (or in some cases all work centers). Upon cessation of the employee's need to access personal data, a letter informing XPI of changes must be submitted within 5 working days.

3.1.2. A current list of personnel authorized access to products containing personal data specifying the range of access, for example, branch data or division data, will be sent to XPI.

3.2. Each supervisor and employee who has access to, prepares input for, or must use computer terminal and/or printed output which have personal data will:

3.2.1. Mark all input with personal data for processing with the phrase “Personal Data - Privacy Act Applies.”

3.2.2. Make sure lists which have the Privacy Act Statement on preprinted forms are properly safeguarded IAW AFI 33-101, *Command, Control, Communications and Computer Systems Management Guidance and Responsibilities.*

3.2.3. Limit access to the products and data to employees who have a specific need for the information to perform their assigned duties.

3.2.4. Record any disclosure of information from the products IAW AFI 37-132.

3.2.5. Shred or tear obsolete listings, including carbon paper, to make them unreadable.

OFFICIAL

CLIFFORD O. ROGERS
Director, Plans and Programs